ITPMG

Helping Companies Improve Their Performance

ITPMG Insights

Asset Management Best Practices

Author: Irv Brownstein

July 2008

IT Performance Management Group

Bethel, CT 06801
+1 203.743.7508

Background

Allowing Users to load personal software, Shareware and the like on a controlled desktop PC opens Pandora's Box to obviate all of the controls and safeguards described in detail throughout this report. More important, this practice places the organization in a state of increased risk from various forms of "mal-ware" as well as a number of potential compliance concerns.

Most organizations of all sizes are moving to greater control over their environment. Typically "Admin" level rights and responsibility is restricted and used to control software modifications to any company asset.

Software Asset Management (SAM)

Software Asset Management (SAM) is the business discipline by which companies optimize investment in software assets by tracking and reconciling installed inventory, measuring the usage of products, and integrating this information with contract and licensing data. Achieving success in SAM is accomplished through the proper integration of people, process, and tools. Software Asset Management choices can impact the entire enterprise. Software has become the fastest growing single IT expenditure and is rapidly becoming one of the largest overall expenses in an organization's budget.

SAM information is essential to operational planning, budgeting, and management. Upgrades, server consolidations, contract negotiations, mergers, divestitures, outsourcing, and insourcing are events that require careful analysis to achieve the most cost effective solution. Without this information, companies are paying for unused, low usage, or out-of-date software, unnecessary hardware upgrades, and avoidable software maintenance fees.

In today's dynamic business environment, having information about your software assets is crucial to making the right decisions. To negotiate the best terms in your software contracts, you need to know where software is actually deployed and how it's being used. With money and capital funding in short supply, the IT organization must clearly show that software investments are contributing to the bottom line. This information is especially useful in competitive replacement negotiations.

There are many advantages and creative ways that companies have found to gain value from a SAM organization. Many of these approaches result in significant direct cost savings and cost avoidance. There are several other benefits that can also have a major cost impact through improved processes and quality factors. Together these form a set of best practices or benefits for SAM that includes:

+1 203.743.7538

- Control Vendor Software Costs
- Contract Compliance and Audits
- Leverage Vendor Contract Negotiations
- Efficient Server Usage and Consolidations
- Improve Operational Performance and Reduce Maintenance Costs
- Invoice Validation
- Reduce Software Fees through Competitive Replacement
- Effective Software and Hardware Upgrades
- Effective Charge-Back
- Disaster Recovery and Business Continuation.

These benefits are significantly reduced or not possible in an uncontrolled IT asset environment.

Compliance Concerns

The Sarbanes-Oxley Act of 2002 is driving the acceptance of SAM as a business discipline. Sarbanes-Oxley is the most sweeping legislation affecting corporate governance, disclosure, and financial accounting in over a generation. This legislation requires an annual evaluation of internal controls and procedures for financial reporting. To be in compliance, a corporation must document its existing controls that bear on financial reporting, test them for efficacy, and report on gaps and deficiencies. An independent auditor must issue a report (to be included in the company's annual report) that attests to management's assertion on the effectiveness of internal controls and procedures and financial reporting.

As a result, IT assets and expenditures (comprised primarily of software expenses) must be controlled, reported on, and effectively managed. Corporate executives can be held directly responsible if they sign documents misstating facts about inventory and use of corporate IT assets. For this reason, many companies have SAM programs being championed by executives who want to be sure that there is a process in place to accurately identify software assets and their efficient use.

The sixth annual Business Software Alliance (BSA) Global Software Piracy Study determined that approximately one out of four software business applications installed on workstations in the United States were unlicensed copies. The study also states that this piracy rate led to approximately $2.6 billion on lost revenues for the US software industry in the same year (and several times that amount worldwide).

Understanding your inventory in relation to your contract information ensures that the software loaded is fully licensed. No company of substantial size can afford the penalties associated with large-scale noncompliance.

Second to the fear of noncompliance in major corporations is the fear of an internal vendor audit. A set of asset management tools combined with a documented SAM

+1 203.743.7538

process can serve as a legal safeguard should there be a compliance issue. Research indicates that compliance law is not as much about strict adherence to the numbers as it is "reasonable effort" to deter piracy. These include "policy definition, written audit procedures, written consequences for noncompliance, and copies of past audits" – all of which require having an asset management solution.

Desktop PC Management

The task of PC management has become too large and too important to be handled on an ad-hoc basis with limited tools. The number of personal computers is significant. There are many versions of operating systems and many different software applications. This is further complicated by the number of employees working from remote offices. The scale has become quite large, even in a small to medium sized business. Now add in the constant stream of

- Software updates (security, operating system and application software updates),
- Periodic operating system upgrades,
- Anti-virus updates, and
- IT configuration changes.

The rate and volume of change is significant and requires ongoing management oversight.

Advances in network bandwidth and the availability of wireless connectivity options have radically increased the number of remote workers, whether working from home or while traveling. The increased use of personal computers and remote access has added significant workload and coordination to the already busy IT schedule. For many knowledge workers, schedules, correspondence, contact lists, presentations and work in progress all live in the desktop.

Most small and medium businesses do not have the IT staff and tools to treat desktop management issues with the attention they deserve. IT shops in small and medium sized companies are generally over-taxed and doing the best they can to keep the IT infrastructure running smoothly. Budgets are much smaller than those of their large enterprise counterparts, staffing is limited, and toolsets are few and far between. Too often manual processes and "just enough to get by" scripting is the answer to desktop management in the small and medium sized company. Individual users can be left to handle minor issues for themselves, and pseudo power users often get themselves into trouble and require IT staff assistance to resolve problems they have created through their self-help efforts. It is no longer a viable answer for small and medium sized business to treat desktop management casually.

The risks of doing a poor job of desktop management are now quite high given the security risks to every PC every day. Left unprotected, PCs are subject to Trojans, Key-loggers, Spyware and Viruses. Every desktop needs Anti-virus software that is constantly updated, and users cannot be trusted to keep their virus data files current.

+1 203.743.7538

Mobile users should also be protected with personal Firewall software, but again, users cannot be depended upon to install and keep such software current. Leaving this to chance can put the entire network and subsequently the entire company at risk.

The employee desktop today contains significant corporate data, both data taken from corporate repositories for use on the desktop as well as work-in-process data not yet stored on a secured and backed-up repository. Employees handle important and sensitive data that needs to be protected. This can include price lists, customer lists, customer data, human resources data, strategic plans, product plans and corporate financial information. Security breaches, viruses, and spyware can lead to stolen, lost or corrupted data. Regular backups can mitigate the risk of lost or corrupted data, however most users are not disciplined enough to perform regular backups. Mobile and remote users complicate the backup problem and render home grown backup scripting ineffective.

Dealing with the disruption and potential data loss of security breaches can represent significant productivity loss. Work-in-process data on the desktop can represent weeks of effort and may be difficult or impossible to recreate. The loss of such data can affect project timelines which in turn can cause customer satisfaction issues and/or contractual penalties. Desktop data loss can also affect revenue if a desktop problem interrupts critical timeframes for customer proposals.

Effective PC Management begins with knowing what you have to manage. Complete and accurate asset and license management is key. Knowing how many machines of what type, their location, memory, hard drive, processor speed, etc., is a big step forward for many small and medium sized businesses. Tools available today have automatic discovery capabilities and excellent management reporting which can assist IT staff in establishing and maintaining good processes for asset management. With an accurate picture of the installed hardware base, it becomes much easier to assess operating system and business suite software upgrades.

With an accurate inventory of all hardware and only the software needed on each desktop, the next step toward effective PC management is to automate software distribution. Automated software distribution minimizes the number of onsite visits IT staff must make. This lowers the cost of support and allows for more frequent updates. This can be applied to virus data files, operating system patches as well as updates and new versions of application software. Changes should be staged in a separate environment for testing and then rolled out based on individual or group user profiles.

Automated software distribution is the first step in remote management. Full remote management includes the ability to remotely control the desktop and make all required configuration changes through a networked connection. This is a critical function as the number of remote and mobile workers has increased. IT staff must be able to perform administrative functions from their office as if they were sitting in front of the PC of remote and mobile workers.

+1 203.743.7538

Another good practice is to keep software installs to the minimum required for each employee to do their job. This will shorten install time, reduce updates and patches required, and use fewer resources leaving more capacity for each user's needs. Again, to accomplish this in an effective manner requires a controlled desktop environment.

The cost of management depends on several factors; the ease-of-use and ease-of-deployment of the management solution, the stability of the environment, the frequency of new releases, and the maturity of the IT organization. Most of these factors translate to IT staff time that is required to manage the management infrastructure. In addition to these direct costs, maintaining a help desk to assist users with PC issues is another additive cost of management. The help desk may be required to operate 24x7, which adds significantly to the cost of ownership.

Desktop Management is a critical business practices that, when done well, can keep employees productive and keep external threats to the company network in check.

To receive additional articles and materials, contact ITPMG at:

information@itpmg.com or

Call 203.743.7538